COVERAGE FOR 'DOOMSDAY OR ARMAGEDDON' DATA BREACH CLASS ACTIONS

24 October 2018 | UK
Legal Briefings – By **Coverage for 'Doomsday or Armageddon' data breach class actions**

Insurance implications of the Court of Appeal's decision to confirm Morrisons' vicarious liability for employee's deliberate actions

We recently updated you on the Court of Appeal's decision in *Wm Morrisons Supermarkets Plc v Various Claimants* [2018] EWCA Civ 233. Click here for our full analysis of the Court of Appeal's decision.

To recap briefly, the Court of Appeal has dismissed an appeal against the High Court's decision that Morrisons was vicariously liable for its employee's misuse of data, despite: (i) Morrisons having done as much as it reasonably could to prevent the misuse; and (ii) the employee's intention being to cause reputational or financial damage to Morrisons itself. It is understood that Morrisons intends to appeal to the Supreme Court.

Companies now find themselves exposed to potential UK data breach class action claims, including for distress-based damages, based on vicarious liability, even if they have appropriate safeguards in place and even if they are the intended victim of the breach. Day by day businesses find themselves responsible for higher volumes of personal data; and the risk of data breach claims is exacerbated by the legislative changes made by the GDPR, increasing public awareness of data protection issues and the publicity that this case has attracted. In addition, the facts of *Morrisons* were such that the company had been found not to be in breach of data protection laws. Future class action claims may be even easier to launch in circumstances where a company has been found to breach the GDPR, for example, by not having appropriate security measures in place.

One of the arguments put forward by Morrisons was that public policy considerations supported an interpretation of the Data Protection Act 1998 which avoids imposing a disproportionate burden on the employer, particularly bearing in mind the difficulty of securing something intangible like data, the potential cost of ensuring compliance and the potential exposure of even small entities to claims for compensation for distress by large numbers of victims (as in the present case), all of which might have a chilling effect on enterprise and efficiency.

The Court of Appeal's response to this concern was to suggest insuring the risk:

"*The solution is to insure against such catastrophes; and employers can likewise insure against losses caused by dishonest or malicious employees. …The fact of a defendant being insured is not a reason for imposing liability, but the availability of insurance is a valid answer to the Doomsday or Armageddon arguments put forward…on behalf of Morrisons*".

This echoes the comments of Mr Justice Langstaff at first instance that many commercial entities will cover the potential losses by appropriate insurance.

Given the court's response to the Doomsday or Armageddon arguments, insurance for data breaches is likely to become more important to policyholders.

There are a number of liability insurance lines that may respond to data breach claims for vicarious liabilities, including most obviously cyber insurance but also potentially data protection cover in general liability insurance, employers' liability insurance, public liability insurance and professional indemnity insurance (where the claims involve financial/professional services breaches). As such, this should not be seen as solely a cyber insurance issue.

A typical cyber insurance policy contains broad cover for data breach claims, together with some costs of managing the incident, making notifications and dealing with regulatory (e.g. ICO) investigations – and potentially also ICO fines in some circumstances. Whilst wordings vary quite significantly both as to scope and legal efficacy, they may well cover vicarious liabilities. That is not to say that claims will be straightforward. There may well be scope for debate on whether insuring clauses are triggered (e.g. on the basis that there is no direct liability or fault of the company) and, even where they are, non-disclosure issues may arise (e.g. in relation to policies and procedures for managing data or cyber risks) or claims might be excluded if sufficiently senior rogue employees were involved - e.g. a director, or an employee colluding with a director, whose intent may be attributed to the company. Further, if the company committed any direct breaches then insurability issues may also arise, particularly where any conduct of the company was deliberate.

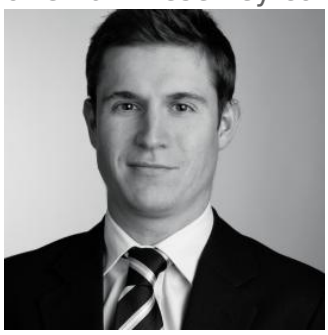
What is less clear is how the market will respond to this enhanced exposure to vicarious liabilities. No doubt the approach will vary between different insurers and different lines. Some insurers may be relatively sanguine if they consider that their current wordings already cover this risk, albeit they may look again at premium levels to ensure the risk is appropriately priced in – particularly if the floodgates open on data breach class action claims. Others may perceive an opportunity, perhaps to extend express coverage or expand their cyber book if appetite from policyholders continues to increase, thus expanding market capacity for these risks in line with current trends in the new data age (again, at an appropriate premium). And yet others, without that appetite, may look to manage their risk by narrowing, excluding or sub-limiting coverage for vicarious liabilities. Of course, many insurers may simply wait and see whether there is a successful appeal to the Supreme Court, if not how the court approaches the issue of quantum and in any event whether Doomsday or Armageddon has been prematurely prophesised.

However the market responds, the golden rule at the placing stage is straightforward: policyholders and insurers should consider in advance whether policies are intended to cover these enhanced risks and ensure that wordings expressly reflect that intention. But that might be easier said than done, particularly where policies provide silent coverage by not excluding cyber or data risks.

It will be interesting to see how this plays out and there may be fertile scope for disputes regarding coverage for data risks going forward, particularly where insurers have not priced in the cover.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



GREIG ANDERSON
PARTNER, LONDON

+44 20 7466 2229
Greig.Anderson@hsf.com

RACHELLE WAXMAN
SENIOR ASSOCIATE, LONDON
+44 20 7466 2400
Rachelle.Waxman@hsf.com

SARAH IRONS
PROFESSIONAL SUPPORT CONSULTANT, LONDON
+44 20 7466 2060
Sarah.Irons@hsf.com

LEGAL NOTICE